PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-285283
(43)Date of publication of application : 12.10.2001

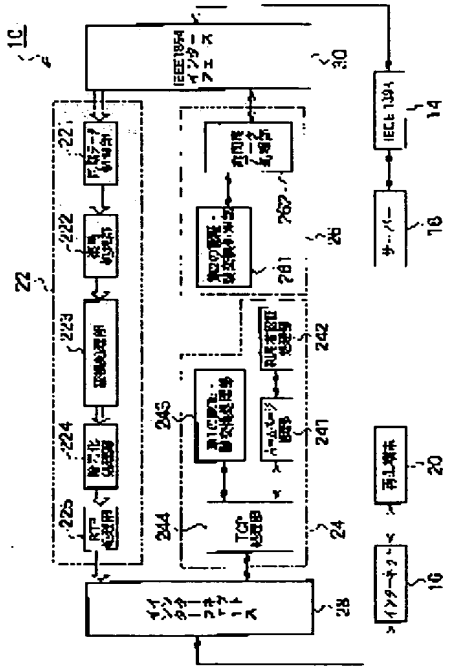
(51)Int.CI. H04L 9/32
G09C 1/00
H04L 9/08
H04L 12/28
H04L 12/66

(21)Application number : 2000-094840
(22)Date of filing : 30.03.2000

(71)Applicant : TOSHIBA CORP
(72)Inventor : SAITO TAKESHI

(54) COMMUNICATION UNIT AND ITS COMMUNICATION METHOD

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a communication unit that can realize protection of copyright in the case of transmitting data from a home network to a public network and to provide its communication method.
SOLUTION: The communication unit interconnects a public network 16 such as the Internet and a home network 14 such as a network in compliance with the IEEE 1394. This communication unit consists of a 1st authentication/key exchange processing section 243 that performs authentication/key exchange with a reproduction terminal 20 connected to the public network 16, a 2nd authentication/key exchange processing section 261 that performs authentication/ key exchange with a server 18 connected to the home network 14, a transmission section 22 that transmits AV data that are encrypted for copyright protection and obtained from the server 18 to the reproduction terminal 20, and a user authentication processing section 242 that authenticates a user of the reproduction terminal 20 and rejects communication with the reproduction terminal 20 when the user cannot be authenticated.



LEGAL STATUS

[Date of request for examination] 20.09.2001
[Date of sending the examiner's decision of rejection] 11.01.2005
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number]
[Date of registration]

[Number of appeal against examiner's decision of rejection] 2005-02443

[Date of requesting appeal against examiner's decision of rejection] 10.02.2005

[Date of extinction of right]

[Claims]

[Claim 1] A communications device which is connected between a first network that is a public network and a second network that is a local area network, and transfers encrypted data between a first terminal connected to the first network and a second terminal connected to the second network, said device comprising:

a first authentication/key exchange unit operable to perform authentication/key exchange with the first terminal;

a second authentication/key exchange unit operable to perform authentication/key exchange with the second terminal;

a transmission unit operable to perform a given conversion of encrypted data obtained from the second terminal, to attach encryption control information identical to or similar to encryption control information attached in advance to the encrypted data, and to transmit to the first terminal; and

a user authentication unit operable to authenticate a user of the first terminal, and when the user cannot be authenticated, to reject communication with the first terminal.

[Claim 2] The communications device according to Claim 1,

wherein said first authentication/key exchange device includes a unit operable to notify the second terminal of a data transmission request for the second terminal from said first terminal.

[Claim 3] The communications device according to Claim 1,

wherein said transmission unit includes:

a unit operable to decrypt the encrypted data obtained from the second terminal;

a unit operable to apply the given conversion to the decrypted data; and

a unit operable to encrypt the converted data.

[Claim 4] The communications device according to Claim 3, which includes

wherein said conversion unit is operable to convert at least one of a data compression encoding method and a data compression encoding speed.

[Claim 5] The communications device according to Claim 1,

wherein said user authentication unit includes

a user information registration unit operable to register, in advance, an identification ID of an authorized user and a password corresponding to the identification ID.

[Claim 6] The communications device according to Claim 2,

wherein said unit operable to notify the second terminal is operable to receive

the data transmission request from the first terminal only in the case where the user of the first terminal has been authenticated.

[Claim 7] The communications device according to Claim 1,

wherein, said first authentication/key exchange unit is operable to perform authentication/key exchange with the first terminal only when the user of the first terminal has been authenticated.

[Claim 8] A communications method of transferring encrypted data between a first terminal connected to a first network that is a public network, and a second terminal connected to a second network that is a local area network, said method comprising:

a process of authenticating a user of the first terminal;

a process of acquiring encrypted data from the second terminal only when the user has been authenticated; and

a process of applying a given conversion to the obtained encrypted data, a process of applying, attaching and transmitting encryption control information that is identical to, or similar, to encryption control information attached to the encrypted data in advance, and to transmit to said first terminal.

[Claim 9] The communications method according to Claim 8,

wherein said process of authenticating the user includes:

a step of acquiring an identification ID from the user and a password which corresponds with the identification ID and,

a step of checking whether or not the acquired identification ID and password match with an already registered identification ID and a password corresponding with the identification ID, of an authorized user.

[Claim 10] The communications method according to Claim 8,

wherein said process of transmitting the encrypted data to the first terminal includes:

a step of decrypting the encrypted data obtained from the second terminal;

a step of applying the given conversion to the decrypted data;

and a step of encrypting the converted data.

[Claim 11]The communications method according to Claim 8 further comprising,

a process of carrying out authentication/key exchange with the first terminal and the second terminal, either before or after said process of acquiring encrypted data from the second terminal.

[Claim 12] The communications method according to Claim 1, further comprising:

an operation which carries out authentication/key exchange with the first terminal either before or after said process of transmitting to the first terminal.

[Claim 13] The communications method according to Claim 8, further comprising

an process of receiving an authentication/key exchange request from the first terminal before or after said process of transmitting to the first terminal; and

a process of performing authentication and key exchange with the first terminal only when the user of the first terminal has been authenticated.

[0011] Further, since the encryption control information such as "No More Copy" etc. which is attached in advance is also attached when transmitted to the playback terminal 20, the original copy control designations can be preserved. Thus also, for example, when data that is specified as not to be recorded and copied is transmitted to playback terminal 20, it can be changed to a format that prevents recording and copying in advance.